DOI: 10.52363/passa-2025.1-14

UDC: 351.74+342.95

Pomaza-Ponomarenko A., *Doctor in Public Administration, Senior Researcher of Science, Head of the research laboratory for studying management problems in the sphere of civil protection, National University of Civil Protection of Ukraine*

ORCID: 0000-0001-5666-9350

PUBLIC GOVERNMENTAL MECHANISMS TO ENSURING CYBER DIPLOMACY AND SAFE DEVELOPMENT OF AI

The theoretical features of the formation of the institution of cyber diplomacy and its role in ensuring the security system in the state are analyzed. The institutional basis for ensuring cyber diplomacy in Estonia is studied. The prospects for the development of the institution of cyber diplomacy in Ukraine are established. Among these prospects, first of all, the revision of the current legal framework of Ukraine in the field of information and cybersecurity, as well as the introduction of the position of Ambassador at Large for Cyber Diplomacy, are identified.

Keywords:*public administration, public administration mechanisms, global security, national security, information security, cybersecurity, cyberdiplomacy, diplomacy, cyberattacks, cyberspace, information infrastructure, artificial intelligence, international law, international terrorism, cyber cadres, digitalization.*

«AI implies institutional Darwinism. Given this, we believe that in the future it is not excluded that the thesis that humans have evolved from AI, and that it is the source of technological fascism, will spread.»

Problem setting. Today, Ukraine is countering an unprecedented number of cyberattacks that accompany unconventional warfare – hybrid warfare. The aggressor state knows why our country has become the object of such attacks. However, the main question that needs to be answered is why our state is becoming a source of new approaches to protecting government systems, and how to use AI, that is, from a security perspective. In our opinion, an important direction for using AI from the perspective of solving security issues is the development of cyber diplomacy in the state. Therefore, it is relevant to determine the prospects for the development of cyber diplomacy in Ukraine and how this type of diplomacy affects global digital security in general. Undoubtedly, the latter requires consideration of the specifics of ensuring cybersecurity. All this determines the relevance of the selected research topic.

Recent research and publications analysis. The issues of guaranteeing and supporting information, digital and cyber security were studied by domestic and foreign scientists S. Belay, O. Bondarenko, U. Vakko, T. Voropaeva, S. Galushko, O. Dovgan, S. Dombrovska, O. Kravchuk, O. Kryukov, E. Magda, F. Miles, V. Matvienko, J. Nye, V. Novikov, O. Parkhomenko-Kutsevil, G. Petushkova, F. Plantera, G. Pocheptsov, O. Radchenko, V. Stepanov, G. Sytnyk, V. Skurativsky, E. Toffler, F. Hoffman, etc. [6; 7; 10]. At the same time, there is a need to detail the prospects for the development of the institute of cyber diplomacy in Ukraine taking into account the requirements of time and society.

Paper objective. The purpose of the article is to determine the features of the formation and implementation of public management mechanisms to ensure cyber diplomacy and the safe development of AI.

Paper main body. At the current stage of development of international relations, the system of public administration is characterized by instability of the institutional environment and rapid growth of challenges and threats. Among this set, a space with two ontological possibilities stands out, the final result of which is not a specific product or phenomenon. This is cyberspace – a living environment that can be both a security challenge and an opportunity for development and cooperation. It is important, given the outlined gender issues, to distinguish between the concepts of «digital diplomacy» and «cyberdiplomacy». If we talk about digital diplomacy, then we are talking primarily about the application of digital technologies to diplomacy, support for diplomatic initiatives, and facilitation of processes through virtual resources. As an example, initiatives to create virtual embassies or simplify consular services for citizens of a state using the Internet. Cyberdiplomacy is the application of diplomacy, namely diplomatic practice, to cyberspace.

The article proceeds from the understanding that cyber diplomacy at the national level is defined as the use of diplomatic instruments and initiatives to ensure the interests of the state in cyberspace. The tasks for a diplomatic agent may be: establishing communication and dialogue between state and non-state actors at different levels; preventing cyber aggression;

developing global norms in cyberspace, etc. Cyber diplomacy is based on the dimensions of soft power and is an effective practice for mitigating uncertainty, eliminating risks and potential conflicts originating from cyberspace. The fundamental elements of cyber diplomacy are increasing cyber potential, strengthening trust, and adhering to and developing cyber norms [6; 7; 11].

However, the main problems in cyberspace or cybersecurity are related to the human factor. They are mostly geopolitical [17]. Disagreements can be traced precisely at the international and national levels. The challenges of cyberspace are about the success of negotiations and political debates on the topic of managing this environment. One of the main problems of cybersecurity is not about how to prevent intrusions, but about the political motivation of individuals and organizations to take responsibility for regulating the components of cybersecurity, as well as how these entities can limit and hold accountable for the malicious activities of an actor in international relations [17].

International law cannot be applied to cyberspace in its entirety and without constant amendments due to the rapid pace of development of information and communication technologies. Currently, the world community has 11 non-binding norms of responsible behavior of states from the UN group of governmental experts. The Tallinn Manual provides clarification on how to apply international law to cyberspace. However, most states have their own concepts and strategic plans that in practice contradict the norms, because they are non-binding. Such classic concepts of international relations as neutrality or arms control do not make sense in cyberspace in their traditional form. The challenge of attribution of cyberattacks is growing in the world community, and there is also a slight fear of escalation between actors due to the unforeseen consequences of cybercrimes.

In cyberspace, the concept of the traditional security dilemma is difficult to apply, since it is almost impossible to distinguish between offensive and defensive operations, especially in relation to international terrorism, which is impossible today without the use of digital technologies. It is difficult for State A to detect the intention of State B, that is, to understand what the purpose of penetration is: to find out the level of protection capabilities, to obtain confidential information, or to conduct one of the stages of intelligence before large-scale cyber operations [6]. In addition, international organizations are also subject to attacks with various purposes of penetration. In the near future, it is the meetings of such organizations to establish and discuss international mandatory standards that will become a geopolitical battlefield, as states will promote their own approaches to managing and protecting cyberspace. Therefore, it is important to involve diplomats in the global development of this environment. Traditional diplomatic skill is gaining importance — the ability to detect the opponent's intentions. The existing approaches of individual regional organizations and integration associations on cybersecurity demonstrate the unification of friends, that is, states with the same vision. In the overall picture of the world order, all these approaches contradict each other. Accordingly, it is necessary to negotiate with potential adversaries and develop a common vision. If the international community aims to expand the effect of cyberspace management from regional, national initiatives to a global unified approach, then it is diplomats who will build norms of international behavior based on best practices. This context implies the need to introduce diplomats into state structures responsible for foreign policy who will develop the geopolitics of cyberspace. It is necessary to focus on rethinking the role of diplomats, reorganizing departments and ministries of foreign affairs in general in order to meet the ever-growing need for cybersecurity specialists in the implementation of foreign policy tasks and rethink the role of new technologies in modern international relations [17].

Given the historical events associated with cyberattacks, as well as the significant potential, supported by leadership among other states in the cybersecurity ranking [1], it is proposed to consider the experience of Estonia, which is only one of the variant models of the possible development of cyber diplomacy in Ukraine. In the early 2000s, Estonia was the first to introduce the concept of "e-Residency": they actively promoted state digital identification, access to the country's electronic services, and a transparent business environment [2].

Estonia has developed a variety of options, including the ability to collect taxes, votes, and health data – all using online platform mechanisms. Despite this innovative approach, in 2007 Estonia suffered the largest cyberattack in its history, as the government, private organizations, the financial sector, television and radio broadcasting, and citizens became targets of the Russian Federation. In 2007, there was no international political mechanism for expert assessment of the consequences of cyberattacks, no procedures for requesting assistance from other states, and no collective condemnation of malicious cyber operations. Since then, Estonia has consistently raised cybersecurity issues both bilaterally and in the UN, EU, NATO, Council of Europe, and beyond. An important step was the establishment in

2008 of the NATO Joint Centre of Excellence for Cyber Defence in Tallinn, which focuses on cyberspace research, training, exchange of ideas, hackathons and operations covering both technical and non-technical components of cyber defence. It is a "think tank" that produces recommendations, organizes conferences and creates an ecosystem of cooperation for both NATO and non-NATO countries.

By the way, Ukraine joined the Joint Center in Tallinn on May 16, 2023. Estonia is a member of the UN Group of Governmental Experts and was a participant in the development of 11 non-binding norms of responsible behavior of states. The country has a unique experience in promoting its own vision of cyberspace on international platforms. Currently, the potential in the cyberspace is being significantly increased due to the fact that Estonia's overall security is supported by NATO, the EU, as well as the well-coordinated activities of the diplomatic corps. It is also important that the idea of the world's first data embassy was implemented in Estonia in 2015. Critical databases and services of Estonia are stored in a high-security data center in Luxembourg, which makes it possible to ensure the digital stability of state authorities even in the event of external threats [8; 18].

In 2018, the Ministry of Foreign Affairs of the Republic of Estonia created the position of Ambassador at Large for Cyber Diplomacy. It took about a decade to finalize this format since the 2007 cyberattacks. In the fall of 2019, the Department of Cyber Diplomacy was established under the jurisdiction of the Ministry of Foreign Affairs of the Republic of Estonia. In 2019, the Department was headed by Ambassador at Large for Cyber Diplomacy Heli Tiirmaa-Klaar [4]. At the time of its establishment, the staff consisted of advisors, as well as officials from the Ministry of Foreign Affairs of the Republic of Estonia who already had relevant experience. During this period, the Ministry also actively demonstrated solidarity with the international community regarding the attribution of cyberattacks. In 2018, it supported the already existing belief that Russian intelligence was involved in the NotPetya and WannaCry cyberattacks directed against international organizations, including the Organization for the Prohibition of Chemical Weapons. It is also important that Estonia clearly defines the responsibilities of the Ministry of Foreign Affairs in cybersecurity strategies. The third Estonian cybersecurity strategy for 2019–2022 aimed to establish a procedure for attribution of cyberattacks [5]; accordingly, on 24 January 2019, the Government approved a guideline (instructions and recommendations) on malicious cyber operations, which clarifies the procedures for providing operational information and contextual analysis. This is necessary for making a political decision on attacks. Depending on the situation, each case, as well as its negative impact, scale and other components, is assessed separately. A working group on attribution issues has been established, which includes representatives of all relevant ministries and departments, including the Ministry of Foreign Affairs.

Estonia is an example of a state that clearly understands the importance of training civil servants in the basics of cyber diplomacy, which is reflected in the creation of the Tallinn Summer School of Cyber Diplomacy, which has been held annually since 2019. The school was organized within the framework of the Multilateralism and Digitalization Program in cooperation with the Ministry of Foreign Affairs of the Republic of Estonia, the Estonian Center for International Development, and the e-Governance Academy [8].

Thus, we see that the Ministry of Foreign Affairs of the Republic of Estonia successfully combines classical diplomatic practices and adapts them to modern realities. The result of this is the creation of the state position of Ambassador at Large for Cyber Diplomacy and a separate department (which has not yet been implemented in Ukraine), as well as the encouragement of training in the basics of cyber diplomacy. It is worth noting that the analysis was carried out as of June 2023 from open sources, we must state the minimal amount of data on cyber diplomacy in Ukraine.

The position of Ambassador at Large for Cyber Diplomacy is not new – more and more countries are opening it within their foreign affairs agencies, and it is important that it is usually a classic government position. Thus, it is a signal that a country is actively involved in this area and is interested in international processes related to cyberspace. It should be emphasized that despite Ukraine’s self-positioning as a state with extensive experience in cybersecurity, it would be appropriate for the Ukrainian Foreign Ministry to act as a global promoter of its potential and the clarification of incidents, as well as to actively participate in the development of international norms. In this context, the issue of improving the current legal framework of Ukraine in the field of information and cybersecurity becomes relevant [14; 15].

Despite the size of Ukraine, a large pool of professional diplomats and higher education institutions where potential internationalists are trained, the Ministry of Foreign Affairs of Ukraine, unlike the Ministry of Foreign Affairs of the Republic of Estonia, does not have a structural unit specialized in cyberspace issues. It is difficult for the average citizen to understand whether there is at least a cyber diplomacy unit within the Department of Public Diplomacy and Communications, or whether it is still a unit in the Directorate of Digital Transformation [11; 12]. The same applies to questions about the presence of a specialist in the position of Ambassador at Large for cyber diplomacy. It is also worth noting the lack of communication in general regarding the state of cyber diplomacy in Ukraine. Such conclusions can be drawn due to the lack of information about this upon inquiries on the official website of the Ministry of Foreign Affairs of Ukraine, pages on social networks of the Ministry of Foreign Affairs of Ukraine and through Google search. Here are some statistics: as of June 30, 2023, the query “cyber diplomacy Ukraine” yielded 827 results, of which every second link minimally covers the subject of the query and does not provide an understanding of the role of the Ministry of Foreign Affairs of Ukraine in cyber diplomacy, its structure, or specialists in this area. The query “Estonia cyber diplomacy” yielded 2,010,000 results that professionally describe the state of cyber diplomacy in Estonia, and the first link – the official page of the Ministry of Foreign Affairs of the Republic of Estonia – aims to familiarize site visitors with the structure, important documents, and vision of cyber diplomacy of the Ministry of Foreign Affairs of Estonia [13]. The query “Ambassador at Large for Cyber Diplomacy at Ministry of Foreign Affairs of Estonia” yielded 163,000 results; however, when viewing the context for a similar query regarding Ukraine, there is no relevant information.

In Ukraine, among the recent public events from which we can draw at least some conclusions about the state of affairs in cyber diplomacy, there is the permanent participation of the advisor to the Ministry of Foreign Affairs of Ukraine on cyber diplomacy in the National Cybersecurity Cluster. Thus, it seems that an information vacuum has been created around the potential and activities in the field of cyber diplomacy in Ukraine. This trend cannot be justified by the concept of “the need for information silence” given the great activity of other entities guaranteeing cybersecurity (the National Cybersecurity Coordination Center, the National Security and Defense Council of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, etc.) in their international activities and publications on the Internet. The question of the reasons for such a situation in the field of cyber diplomacy will probably remain debatable for some time to come – conditionally based on the time frame, starting from active cyberattacks in 2014 and continuing with their peak, which coincided with the beginning of full-scale aggression by the Russian Federation. It should be noted that Ukraine's task is to prevent the development of AI as another technological fascism.

Conclusions. Given the information bubble, the small percentage of specialists involved in discussing the future of Ukrainian cyber diplomacy, and the lack of encouragement for the vertical from top to bottom, we have: 1. A small number of human resources who can potentially hold diplomatic positions and at the same time be experts in cyber issues. 2. A low level of professional and scientific interest in cyber diplomacy. This state of affairs is caused by the fact that, against the background of other challenges, the professional community places this area, at best, no higher than second place in the ranking of priority problems to be solved. Additionally, this issue is usually highlighted by the lack of platforms for exchanging views.

We believe that cyber diplomacy currently has a large set of opportunities for training, platforms for discussions, scientific and practical conferences, etc. It is necessary to be able to periodically hold an open discussion of current problems of cyber diplomacy with the participation of experts, scientists and relevant institutions under the leadership of the Ministry of Foreign Affairs of Ukraine. Such an initiative will provide an impetus for the exchange of ideas and practices regarding possible options for development, overcoming crises or building cooperation, promoting national narratives in the international arena in the field of cyber diplomacy. Referring to the Cybersecurity Strategy of Ukraine from 2021 [14], we see a desire for partnership, primarily with the EU, NATO, the USA and other states, based on interaction, in which one of the priorities is precisely the development of the institution of cyber diplomacy in the domestic territory.

References:

1. National Cyber Security Index (no date). Available at: https://ncsi.ega.ee/ncsi-index/?order=-ncsi (Accessed: 20 May 2025).

2. e-Estonia (no date) This is the story of the world's most advanced digital society. Available at: https://e-estonia. com/story/ (Accessed: 30 May 2025).

3. Pomaza-Ponomarenko A., Kryvova S., Hordieiev A., Hanzyuk A., Halunko O. Innovative Risk Management: Identification, Assessment and Management of Risks in the Context of Innovative Project Management // Economic Affairs (New Delhi). 2023, 68(4), pp. 2263–2275.

DOI: 10.46852/0424-2513.4.2023.34. URL: https://ndpublisher.in/admin/issues/EAv68n5z8.pdf.

4. e-Estonia (2019) Estonia takes on a major role in cyber diplomacy with a new department for international cooperation. Available at: https://e-estonia.com/estonia-cyber-diplomacy-international-cooperation/ (Accessed: 30 May 2025).

5. Ministry of Economic Affairs and Communications of Estonia (2019) Cybersecurity Strategy Republic of Estonia. Available at: https://www.mkm.ee/media/703/download (Accessed: 20 May 2025).

6. Novikov V. Approaches to improvement of the institutional system and mechanisms of public administration in the conditions of information-hybrid wars // Eurasian Academic Research Journal. 2020. Vol. 37. Pp. 75–80.

7. Halushko S. Typology of digital technologies and their socio-political and state-legal effects on the sphere of national security // Public administration and state security aspects. 2024. Vol. 1. pp. 15–32.

8. Delegation of the European Union to the Kingdom of Lesotho (2023) Welcome to the Tallinn Summer School of Cyber Diplomacy. Available at: https://www.eeas.europa.eu/delegations/lesotho/welcome-tallinn-summer-school-cyber-diplomacy_en?s=103 (Accessed: 29 May 2025).

9. e-Governance Academy (2023) The Tallinn Summer School of Cyber Diplomacy brought together participants from 43 countries. Available at: https://ega.ee/news/tallinn-summer-school-cyber-diplomacy-participants/ (29 May 2025).

10. Plantera, F. (2023) Cyber diplomats from all around the globe will soon gather in Tallinn [Podcast]. 6 June. Available at: https://ega.ee/blog_post/cyber-diplomacy (Accessed: 30 May 2025).

11. Dombrovska S.M., Pomaza-Ponomarenko A.L., Kryukov O.I., Poroka S.G. Information threats and communication infrastructure in the state sector: monograph. Kharkiv: NUCZU, 2024. 244 p. URL: http://repositsc.nuczu.edu.ua/handle/123456789/19990 (Accessed: 30 May 2025).

12. Structural divisions // Ministry of Foreign Affairs of Ukraine. URL: https://mfa.gov.ua/pro-ministerstvo/ struktura/struktrunni-pidrozdili

13. Ministry of Foreign Affairs of Estonia (2023) Cyber diplomacy. Available at: https://

www.vm.ee/en/international-law-cyber-diplomacy/cyber-diplomacy (Accessed: 30 May 2025).

14. On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 “On the Cybersecurity Strategy of Ukraine”: Decree of the President of Ukraine No. 447/2021 dated 08/26/2021. URL: https://www.president. gov.ua/documents/4472021-40013 (Accessed: 30 May 2025).

15. On the Implementation Plan of the Cybersecurity Strategy of Ukraine: Decision of the National Security and Defense Council of Ukraine dated 12/30/2021. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text (Accessed: 29 May 2025).

16. Lopatchenko I.M., Pomaza-Ponomarenko A.L., Batyr Y.Yu. State regulation in the sphere of information security of Ukraine under martial law // Bulletin of the National University of Civil Defense of Ukraine (Series «State Administration»). 2024. No. 1 (20). P. 14–24.

Pomaza-Ponomarenko A.L., Taraduda D.V. Service and combat activities of law enforcement forces and international humanitarian law // State Administration: improvement and development. 2024. No. 3. URL: https://www.nayka.com.ua/index.php/dy/article/view/3229.

EU Sanctions Map (2023). Available at: https://www.sanctionsmap.eu/#/main (Accessed: 29 May 2025).